PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-366525

(43)Date of publication of application : 20.12.2002

(51)Int.Cl. G06F 15/00

(21)Application number : 2001-215975

(22)Date of filing : 12.06.2001

(71)Applicant : NEEDS CREATOR KK

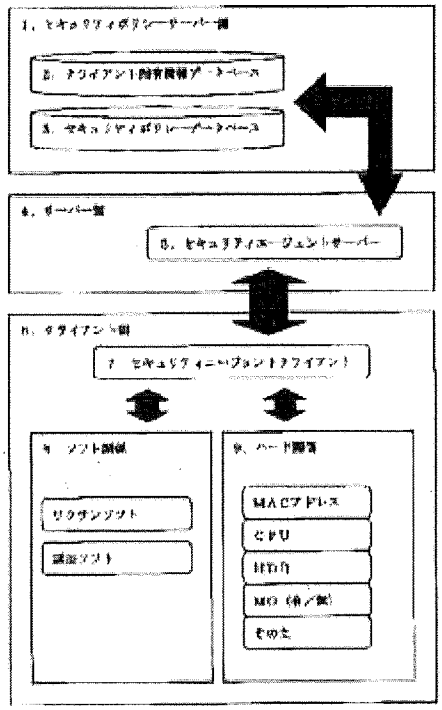
(72)Inventor : KOSHIDA TOSHIO

(54) SECURITY POLICY MAINTENANCE SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To newly develop a system for maintaining the security policy of a network.

SOLUTION: When a client 6 logs in a network, resource information of the client is acquired by a security agent client 7, transmitted to a security agent server 5, an information data base 2 intrinsic to the client is compared with a security policy data base 3 in a security policy server 1 and permission or nonpermission of network log in by the client 6 is determined. In addition, the security agent client 7 always monitors an operating state of the client 6, transmits it to the security agent server 5 and when breach of the security policy is caused, disconnects network connection by the client 6.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号
特開2002－366525
（P2002－366525A）
(43)公開日　平成14年12月20日(2002.12.20)

(51)Int.Cl.'	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｄ　５Ｂ０８５
	３２０		３２０Ｋ

審査請求　未請求　請求項の数３　書面　（全　４　頁）

(21)出願番号　特願2001－215975(P2001－215975)

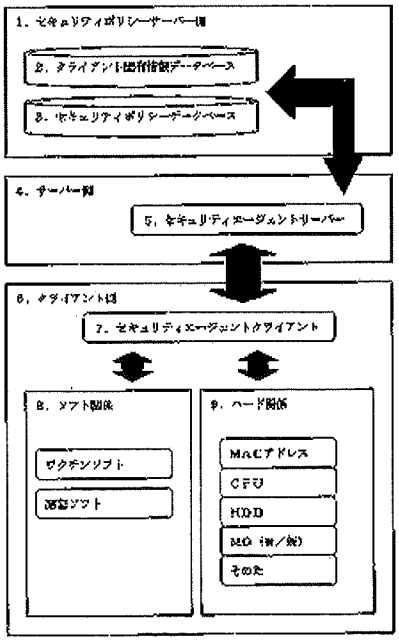
(22)出願日　平成13年６月12日(2001.6.12)

(71)出願人　501082336
ニーズクリエイター株式会社
福岡県福岡市中央区高砂１丁目21番11号
(72)発明者　越田　敏臣
福岡県福岡市中央区高砂１丁目21－11　ニーズクリエイター株式会社内

Ｆターム(参考)　5B085 AC01 AC11 AE00 BA07 BC07

(54)【発明の名称】　セキュリティポリシー維持システム

(57)【要約】
【課題】ネットワークのセキュリティポリシーを維持するシステムが無かった
【解決手段】６のクライアントがネットワークにログインする際に、７のセキュリティエージェントクライアントにて、クライアントのリソース情報を取得し、５のセキュリティエージェントサーバーに送信され、１のセキュリティポリシーサーバー内の、２のクライアント固有情報データベースと３のセキュリティポリシーデータベースと比較し、６のクライアントのネットワークログイン許可または不許可を判断する。また、７のセキュリティエージェントクライアントは、常時６のクライアントの動作状況を監視、５のセキュリティエージェントサーバーに送信し、セキュリティポリシー違反が発生した場合、６のクライアントのネットワーク接続を切断する・



1

【特許請求の範囲】

【請求項１】　ネットワークに参加するクライアントのセキュリティレベルにより，サーバー側よりクライアントのネットワーク参加を許可および拒否する手段と，前記のセキュリティレベル情報を取得し，クライアントとサーバー間でのセキュリティレベルの確認手段と，を備えたことを特徴とする，セキュリティポリシー維持管理装置やアプリケーションとそれを記録する媒体

【請求項２】　クライアントがネットワークに参加し，処理を継続している間も，クライアントのセキュリティレベル情報を監視し，セキュリティレベルがネットワーク参加可能レベルより低くなった場合やセキュリティレベル情報の取得が出来なくなった場合にネットワーク資源の利用を制限する手段とを備えたことを特徴とする，メール管理装置やアプリケーションとそれを記録する媒体

【請求項３】ネットワーク管理者が許可した正規クライアントと無許可のクライアントの判断手段とを備えたことを特徴とする，セキュリティポリシー維持管理装置やアプリケーションとそれを記録する媒体

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は，コンピュータネットワークの利用においてネットワークに参加するクライアントセキュリティレベルにより，ネットワークセキュリティレベル管理制御装置やアプリケーションとそれを記録する媒体に関するものである。

【０００２】

【従来の技術】従来は，コンピュータネットワークを構築し運用していく場合は，事前に運用マニュアル等を作成し，その中でセキュリティ維持の為の項目を設定し，利用者のモラルの向上を行い，セキュリティレベルを維持していた。

【０００３】また，ネットワーク参加者の区別は，ネットワークログインＩＤとパスワードのみチェックで参加を許可していた為，プライベートパソコンや取り決めたセキュリティレベルを維持していないクライアントも，簡単にネットワークに参加していた。

【０００４】また，ネットワーク管理者が知らないセキュリティレベルの低いクライアントが数多くネットワークに参加する事で，ネットワークのセキュリティレベルが低下し，ウィルスへの感染や情報の漏洩などの重大な問題が発生する場合があった。

【０００５】

【発明が解決しようとする課題】本発明は，前記の課題を解決する為に，クライアントのセキュリティレベル情報取得と取得したセキュリティレベルによりネットワークへの参加を拒否および制限を行うことが出来る様にしたもので，以下の装置および方法を特徴とする。

【０００６】本発明の目的は，ネットワーク管理者が定めたセキュリティレベルの基準に至らないクライアントのネットワーク参加を制限する管理方法を提供することにある。

2

【０００７】

【課題を解決する為の手段】サーバーとクライアントにセキュリティチェックエージェントを常駐させ，クライアントの電源を入れ，起動した時点からセキュリティエージェントが起動する。そのセキュリティエージェントは，クライアント上にネットワーク管理者が設定した，常時正常動作が必要なアプリケーションの稼動状況とバージョン情報の取得を行う。また，その他の稼動中アプリケーション情報の取得を行い，取得した情報をログイン処理と共にサーバーに伝送する。

【０００８】サーバー側は，伝送されたクライアントセキュリティ情報および，クライアントのＭＡＣアドレスやＣＰＵおよびＨＤＤサイズ等の固有データをセキュリティポリシー設定データベースの内容と比較し，ネットワーク参加の可否を判断する。

【０００９】ネットワーク参加が許可された場合は，ネットワーク資源を利用する事が出来る様になるが，不許可の場合は，ネットワークログインを拒否する。

【００１０】また，前記のセキュリティエージェントが稼動していないクライアントからネットワークサーバーにログイン処理が行われた場合は，サーバー側に常駐しているセキュリティエージェントにより，ネットワークログイン処理を強制的に中断し，ネットワーク参加を拒否する。

【００１１】

【発明の実施の形態】ネットワーク利用者は，自己の管理している６のクライアントを起動し，起動後ＩＤとパスワードを入力して，ネットワークにログインする。

【００１２】前記のクライアントが，正規許可のクライアント場合は，７のセキュリティエージェントクライアントにより，８のソフト稼動状況や９のハードリソース情報が取得され，ログイン処理と共に７のセキュリティエージェントクライアントから５のセキュリティエージェントサーバーに送られ，６のセキュリティエージェントサーバーは，１のセキュリティポリシーサーバー上の，２のクライアント固有情報データベースと３のセキュリティポリシーデータベース情報を元に，ログインの可否を判断する。

【００１３】セキュリティレベルが基準に達していれば，５のセキュリティエージェントサーバーは，７のセキュリティエージェントクライアントに対し，ログインを許可する。

【００１４】しかし，セキュリティレベルが基準以下の場合，５のセキュリティエージェントサーバーは，７のセキュリティエージェントクライアントに対し，ログインを拒否し，ログインの拒否理由を７のセキュリティエージェントクライアントに送信する。７のセキュリティ

エージェントクライアントは、受信した拒否理由を表示しする。利用者は指示に従って対処し、再度ログイン処理を行う。

【００１５】また、個人所有の正規許可のクライアントで無い場合は、７のセキュリティエージェントクライアントが稼動していなか、または稼動していてもＭＡＣアドレスやＣＰＵおよびＨＤＤサイズとうのクライアント固有の情報が、２のクライアント固有情報データベースに登録が無い為、５のセキュリティエージェントサーバーにより、ネットワーク参加が拒否される。

【００１６】また、７のセキュリティエージェントクライアントは、ネットワークに接続中に、６のクライアントのソフトやハードのリソースに変化を検知し、５のセキュリティエージェントサーバーに通知する、５のセキュリティエージェントサーバーは、通知内容がセキュリティポリシーデータベースと比較し、セキュリティポリシーに違反があれば、６のクライアントをネットワークより強制的に切断する。

【００１７】また、５のセキュリティエージェントサーバーは、常時７のセキュリティエージェントクライアントの動作を監視し、７のセキュリティエージェントクライアントからの信号が途絶えた場合、６のクライアントのセキュリティレベルに異常が発生したと判断し、ネットワークより強制的に切断する。

【００１８】

【発明の効果】本発明のセキュリティポリシー維持システムを利用する事で、セキュリティポリシーに違反するクライアントの接続を防止し、ネットワークのセキュリティレベルを維持できる。また、各クライアントのリソース状況をデータベースに記録し管理することで、悪意を持ってＭＯやＲＡＳ環境増設を行っても、ネットワークから自動的に切り離される為、機密情報や個人情報の漏洩やウィルスの侵入を防止することができる。

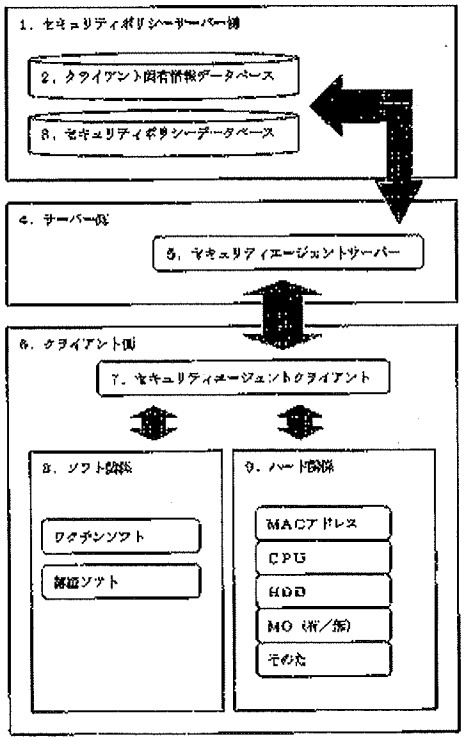
【図面の簡単な説明】

【図１】本発明の基本処理の流れを説明した図である

【符号の説明】

１　－　セキュリティポリシーサーバー
２　－　クライアント固有情報データベース
３　－　セキュリティポリシーデータベース
４　－　サーバー
５　－　セキュリティエージェントサーバー
６　－　クライアント
７　－　セキュリティエージェントクライアント
８　－　ソフト関係
９　－　ハード関係

【図１】



【手続補正書】
【提出日】平成１３年７月２３日（２００１．７．２３）
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】請求項２
【補正方法】変更
【補正内容】
【請求項２】　クライアントがネットワークに参加し、処理を継続している間も、クライアントのセキュリティレベル情報を監視し、セキュリティレベルがネットワーク参加可能レベルより低くなった場合やセキュリティレベル情報の取得が出来なくなった場合にネットワーク資源の利用を制限する手段とを備えたことを特徴とする、セキュリティポリシー維持管理装置やアプリケーションとそれを記録する媒体
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】発明の属する技術分野
【補正方法】変更
【補正内容】
【発明の属する技術分野】本発明は、コンピュータネットワークの利用においてネットワークに参加するクライアントセキュリティレベルにより、ネットワーク参加を制限する装置やアプリケーションとそれを記録する媒体に関するものである。